



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/733,320

12/12/2003

Robert Joseph Harley

021185-000200US

9086

20350 7590 06/18/2008  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

EXAMINER

JOHNSON, CARLTON

ART UNIT

PAPER NUMBER

2136

MAIL DATE

DELIVERY MODE

06/18/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<p align="center"><b>Advisory Action</b> <b>Before the Filing of an Appeal Brief</b></p>	<p><b>Application No.</b> 10/733,320</p>	<p><b>Applicant(s)</b> HARLEY, ROBERT JOSEPH</p>	
	<p><b>Examiner</b> CARLTON V. JOHNSON</p>	<p><b>Art Unit</b> 2136</p>	

**--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

THE REPLY FILED 02 June 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
- b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on \_\_\_\_\_. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

#### AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
- (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
- (b) ☐ They raise the issue of new matter (see NOTE below);
- (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
- (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: \_\_\_\_\_. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): \_\_\_\_\_.
6. ☐ Newly proposed or amended claim(s) \_\_\_\_\_ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
- The status of the claim(s) is (or will be) as follows:
- Claim(s) allowed: \_\_\_\_\_.
- Claim(s) objected to: \_\_\_\_\_.
- Claim(s) rejected: 1-15.
- Claim(s) withdrawn from consideration: \_\_\_\_\_.

#### AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

#### REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:  
See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). \_\_\_\_\_
13. ☐ Other: \_\_\_\_\_.

/Nasser G Moazzami/  
Supervisory Patent Examiner, Art Unit 2136

/Carlton V. Johnson/  
Examiner, Art Unit 2136

Continuation of 11. does NOT place the application in condition for allowance because: 10733320:  
Response to Remarks

The amended claims will not be entered.

The amendments have changed the scope of claim 1 and its dependent claims 2 - 11. The amendments changed the claim limitation from "the number of points" to the "total number of points".

The USPTO has rules which state that a system that is comprised strictly of software is non-statutory. Unless the applicant can disclose a hardware component for the system, then the system has to be rejected using USC 101. The specification in paragraph [40] discloses "steps or functions described herein can be performed in hardware, software, or a combination of the two." In the broadest possible terms, the system can be embodied in software only. Perhaps this statement should be: "steps or functions described herein can be performed in a combination of hardware and software". The 112 rejection stands since the specification has not been corrected.

The 112 rejection is a 1st paragraph or a 2nd paragraph rejection?

The 112 rejections in question should have been USC 112 1st paragraph rejections. The claim limitations: "determining the number of points on the elliptic curve, wherein the determining includes solving a lifted Frobenius equation to a full precision by using first and second parts with a reduced precision"; "a second phase computes a norm to determine the number of points on the curve as output"; and "lifted Frobenius" were not disclosed within the specification. Perhaps these indicated references should be listed as IDS references and placed in the record as prior art. (Sat2000, FGH2000)

There is no disclosure of a lifted Frobenius equation in the specification or the original claims which can be used in a determination of the number of points on an elliptical curve. (see USC 112 Rejection) The specification does disclose canonical lift which is addressed in a separate claim limitation (claim 4). The Hoffstein prior art discloses calculations with Frobenius equations and elliptic curves. Hoffstein prior art discloses a way to count points of a curve. (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: using elliptic curves)

The basis for the claimed invention is a sequence of mathematical calculations based on algorithms or equations. All of the referenced prior art (Hoffstein, Gressel, Penner) are in the same field of endeavor as the claimed invention, mathematical calculations using algorithms arithmetic operations.